LPI 303-200

LPI LPIC-3 303 Certification Questions & Answers

Exam Summary – Syllabus –Questions

303-200
LPIC-3 Security
60 Questions Exam – 500/800 Cut Score – Duration of 90 minutes

Table of Contents:

Know Your 303-200 Certification Well:

The 303-200 is best suitable for candidates who want to gain knowledge in the LPI Linux System Administration. Before you start your 303-200 preparation you may struggle to get all the crucial LPIC-3 303 materials like 303-200 syllabus, sample questions, study guide.

But don't worry the 303-200 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the 303-200 syllabus?
- How many questions are there in the 303-200 exam?
- Which Practice test would help me to pass the 303-200 exam at the first attempt?

Passing the 303-200 exam makes you LPIC-3 Security. Having the LPIC-3 303 certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

LPI 303-200 LPIC-3 303 Certification Details:

Exam Name	LPIC-3 Security
Exam Code	303-200
Exam Price	$200 (USD)
Duration	90 mins
Number of Questions	60
Passing Score	500 / 800
Schedule Exam	**LPI Marketplace**
Sample Questions	**LPI LPIC-3 Sample Questions**
Practice Exam	**LPI 303-200 Certification Practice Exam**

303-200 Syllabus:

Topic	Details
Cryptography	
X.509 Certificates and Public Key Infrastructures	**Weight:** 5 **Description:** Candidates should understand X.509 certificates and public key infrastructures. They should know how to configure and use OpenSSL to implement certification authorities and issue SSL certificates for various purposes. **Key Knowledge Areas:** - Understand X.509 certificates, X.509 certificate lifecycle, X.509 certificate fields and X.509v3 certificate extensions - Understand trust chains and public key infrastructures - Generate and manage public and private keys - Create, operate and secure a certification authority - Request, sign and manage server and client certificates - Revoke certificates and certification authorities **The following is a partial list of the used files, terms and utilities:** - openssl, including relevant subcommands - OpenSSL configuration - PEM, DER, PKCS - CSR - CRL - OCSP
X.509 Certificates for Encryption, Signing and Authentication	**Weight:** 4 **Description:** Candidates should know how to use X.509 certificates for both server and client authentication. Candidates should be able to implement user and server authentication for Apache HTTPD. The version of Apache HTTPD covered is 2.4 or higher. **Key Knowledge Areas:** - Understand SSL, TLS and protocol versions - Understand common transport layer security threats, for example Man-in-the-Middle - Configure Apache HTTPD with mod_ssl to provide HTTPS service, including SNI and HSTS

Topic	Details
	- Configure Apache HTTPD with mod_ssl to authenticate users using certificates - Configure Apache HTTPD with mod_ssl to provide OCSP stapling - Use OpenSSL for SSL/TLS client and server tests **Terms and Utilities:** - Intermediate certification authorities - Cipher configuration (no cipher-specific knowledge) - httpd.conf - mod_ssl - openssl
Encrypted File Systems	**Weight:** 3 **Description:** Candidates should be able to setup and configure encrypted file systems. **Key Knowledge Areas:** - Understand block device and file system encryption - Use dm-crypt with LUKS to encrypt block devices - Use eCryptfs to encrypt file systems, including home directories and - PAM integration - Be aware of plain dm-crypt and EncFS **Terms and Utilities:** - cryptsetup - cryptmount - /etc/crypttab - ecryptfsd - ecryptfs-* commands - mount.ecryptfs, umount.ecryptfs - pam_ecryptfs
DNS and Cryptography	**Weight:** 5 **Description:** Candidates should have experience and knowledge of cryptography in the context of DNS and its implementation using BIND. The version of BIND covered is 9.7 or higher. **Key Knowledge Areas:** - Understanding of DNSSEC and DANE - Configure and troubleshoot BIND as an authoritative name server serving DNSSEC secured zones - Configure BIND as an recursive name server that performs DNSSEC validation on behalf of its clients

Topic	Details
	- Key Signing Key, Zone Signing Key, Key Tag - Key generation, key storage, key management and key rollover - Maintenance and re-signing of zones - Use DANE to publish X.509 certificate information in DNS - Use TSIG for secure communication with BIND **Terms and Utilities:** - DNS, EDNS, Zones, Resource Records - DNS resource records: DS, DNSKEY, RRSIG, NSEC, NSEC3, NSEC3PARAM, TLSA - DO-Bit, AD-Bit - TSIG - named.conf - dnssec-keygen - dnssec-signzone - dnssec-settime - dnssec-dsfromkey - rndc - dig - delv - openssl
Host Security	
Host Hardening	**Weight:** 3 **Description:** Candidates should be able to secure computers running Linux against common threats. This includes kernel and software configuration. **Key Knowledge Areas:** - Configure BIOS and boot loader (GRUB 2) security - Disable useless software and services - Use sysctl for security related kernel configuration, particularly ASLR, Exec-Shield and IP / ICMP configuration - Exec-Shield and IP / ICMP configuration - Limit resource usage - Work with chroot environments - Drop unnecessary capabilities - Be aware of the security advantages of virtualization **Terms and Utilities:** - grub.cfg - chkconfig, systemctl

Topic	Details
	- ulimit - /etc/security/limits.conf - pam_limits.so - chroot - sysctl - /etc/sysctl.conf
Host Intrusion Detection	**Weight:** 4 **Description:** Candidates should be familiar with the use and configuration of common host intrusion detection software. This includes updates and maintenance as well as automated host scans. **Key Knowledge Areas:** - Use and configure the Linux Audit system - Use chkrootkit - Use and configure rkhunter, including updates - Use Linux Malware Detect - Automate host scans using cron - Configure and use AIDE, including rule management - Be aware of OpenSCAP **Terms and Utilities:** - auditd - auditctl - ausearch, aureport - auditd.conf - auditd.rules - pam_tty_audit.so - chkrootkit - rkhunter - /etc/rkhunter.conf - maldet - conf.maldet - aide - /etc/aide/aide.conf
User Management and Authentication	**Weight:** 5 **Description:** Candidates should be familiar with management and authentication of user accounts. This includes configuration and use of NSS, PAM, SSSD and Kerberos for both local and remote directories and authentication mechanisms as well as enforcing a password policy.

Topic	Details
	Key Knowledge Areas: - Understand and configure NSS - Understand and configure PAM - Enforce password complexity policies and periodic password changes - Lock accounts automatically after failed login attempts - Configure and use SSSD - Configure NSS and PAM for use with SSSD - Configure SSSD authentication against Active Directory, IPA, LDAP, Kerberos and local domains - Kerberos and local domains - Obtain and manage Kerberos tickets **Terms and Utilities:** - nsswitch.conf - /etc/login.defs - pam_cracklib.so - chage - pam_tally.so, pam_tally2.so - faillog - pam_sss.so - sssd - sssd.conf - sss_* commands - krb5.conf - kinit, klist, kdestroy
FreeIPA Installation and Samba Integration	**Weight:** 4 **Description:** Candidates should be familiar with FreeIPA v4.x. This includes installation and maintenance of a server instance with a FreeIPA domain as well as integration of FreeIPA with Active Directory. **Key Knowledge Areas:** - Understand FreeIPA, including its architecture and components - Understand system and configuration prerequisites for installing FreeIPA - Install and manage a FreeIPA server and domain - Understand and configure Active Directory replication and Kerberos cross-realm trusts - Be aware of sudo, autofs, SSH and SELinux integration in FreeIPA **Terms and Utilities:** - 389 Directory Server, MIT Kerberos, Dogtag Certificate System, NTP, DNS, SSSD, certmonger

Topic	Details
	- ipa, including relevant subcommands - ipa-server-install, ipa-client-install, ipa-replica-install - ipa-replica-prepare, ipa-replica-manage
Access Control	
Discretionary Access Control	**Weight:** 3 **Description:** Candidates are required to understand Discretionary Access Control and know how to implement it using Access Control Lists. Additionally, candidates are required to understand and know how to use Extended Attributes. **Key Knowledge Areas:** - Understand and manage file ownership and permissions, including SUID and SGID - Understand and manage access control lists - Understand and manage extended attributes and attribute classes **Terms and Utilities:** - getfacl - setfacl - getfattr - setfattr
Mandatory Access Control	**Weight:** 4 **Description:** Candidates should be familiar with Mandatory Access Control systems for Linux. Specifically, candidates should have a thorough knowledge of SELinux. Also, candidates should be aware of other Mandatory Access Control systems for Linux. This includes major features of these systems but not configuration and use. **Key Knowledge Areas:** - Understand the concepts of TE, RBAC, MAC and DAC - Configure, manage and use SELinux - Be aware of AppArmor and Smack **Terms and Utilities:** - getenforce, setenforce, selinuxenabled - getsebool, setsebool, togglesebool - fixfiles, restorecon, setfiles - newrole, runcon

Topic	Details
	- semanage - sestatus, seinfo - apol - seaudit, seaudit-report, audit2why, audit2allow - /etc/selinux/*
Network File Systems	**Weight:** 3 **Description:** Candidates should have experience and knowledge of security issues in use and configuration of NFSv4 clients and servers as well as CIFS client services. Earlier versions of NFS are not required knowledge. **Key Knowledge Areas:** - Understand NFSv4 security issues and improvements - Configure NFSv4 server and clients - Understand and configure NFSv4 authentication mechanisms (LIPKEY, SPKM, Kerberos) - Understand and use NFSv4 pseudo file system - Understand and use NFSv4 ACLs - Configure CIFS clients - Understand and use CIFS Unix Extensions - Understand and configure CIFS security modes (NTLM, Kerberos) - Understand and manage mapping and handling of CIFS ACLs and SIDs in a Linux system **Terms and Utilities:** - /etc/exports - /etc/idmap.conf - nfs4acl - mount.cifs parameters related to ownership, permissions and security modes - winbind - getcifsacl, setcifsacl
Network Security	
Network Hardening	**Weight:** 4 **Description:** Candidates should be able to secure networks against common threats. This includes verification of the effectiveness of security measures. **Key Knowledge Areas:** - Configure FreeRADIUS to authenticate network nodes

Topic	Details
	- Use nmap to scan networks and hosts, including different scan methods - Use Wireshark to analyze network traffic, including filters and statistics - Identify and deal with rogue router advertisements and DHCP messages **Terms and Utilities:** - radiusd - radmin - radtest, radclient - radlast, radwho - radiusd.conf - /etc/raddb/* - nmap - wireshark - tshark - tcpdump - ndpmon
Network Intrusion Detection	**Weight:** 4 **Description:** Candidates should be familiar with the use and configuration of network security scanning, network monitoring and network intrusion detection software. This includes updating and maintaining the security scanners. **Key Knowledge Areas:** - Implement bandwidth usage monitoring - Configure and use Snort, including rule management - Configure and use OpenVAS, including NASL **Terms and Utilities:** - ntop - Cacti - snort - snort-stat - /etc/snort/* - openvas-adduser, openvas-rmuser - openvas-nvt-sync - openvassd - openvas-mkcert - /etc/openvas/*
Packet Filtering	**Weight:** 5

Topic	Details
	Description: Candidates should be familiar with the use and configuration of packet filters. This includes netfilter, iptables and ip6tables as well as basic knowledge of nftables, nft and ebtables. **Key Knowledge Areas:** - Understand common firewall architectures, including DMZ - Understand and use netfilter, iptables and ip6tables, including standard modules, tests and targets - Implement packet filtering for both IPv4 and IPv6 - Implement connection tracking and network address translation - Define IP sets and use them in netfilter rules - Have basic knowledge of nftables and nft - Have basic knowledge of ebtables - Be aware of conntrackd **Terms and Utilities:** - iptables - ip6tables - iptables-save, iptables-restore - ip6tables-save, ip6tables-restore - ipset - nft - ebtables
Virtual Private Networks	**Weight:** 4 **Description:** Candidates should be familiar with the use of OpenVPN and IPsec. **Key Knowledge Areas:** - Configure and operate OpenVPN server and clients for both bridged and routed VPN networks - Configure and operate IPsec server and clients for routed VPN networks using IPsec-Tools / racoon - Awareness of L2TP **Terms and Utilities:** - /etc/openvpn/* - openvpn server and client - setkey - /etc/ipsec-tools.conf - /etc/racoon/racoon.conf

LPI 303-200 Sample Questions:

Question: 1

What happens when the command getfattr afile is run while the file afile has no extended attributes set?

a) getfattr prints a warning and exits with a values of 0.
b) No output is produced and getfattr exits with a value of 0.
c) getfattr prints a warning and exits with a value of 1.
d) No outputs is produced and getfattr exits with a value of 1.

Answer: b

Question: 2

An X509 certificate contains the following information:

X509v3 Basic Constraints: critical CA:TRUE, pathlen:0

Which of the following statements are true regarding the certificate?

(Choose THREE correct answers.)

a) This certificate belongs to a certification authority.
b) This certificate may be used to sign certificates of subordinate certification authorities.
c) This certificate may never be used to sign any other certificates.
d) This certificate may be used to sign certificates that are not also a certification authority.
e) This certificate will not be accepted by programs that do not understand the listed extension.

Answer: a, b, d

Question: 3

In which path is the data, which can be altered by the sysctl command, accessible?

a) /dev/sys/
b) /sys/
c) /proc/sys/
d) /sysctl/

Answer: c

Question: 4

What effect does the configuration SSLStrictSNIVHostCheck on have on an Apache HTTPD virtual host?

a) Despite its configuration, the virtual host is served only on the common name and Subject Alternative Names of the server certificates.
b) The virtual host is used as a fallback default for all clients that do not support SNI.
c) All of the names of the virtual host must be within the same DNS zone.
d) The virtual host is served only to clients that support SNI.
e) The clients connecting to the virtual host must provide a client certificate that was issued by the same CA that issued the server's certificate.

Answer: d

Question: 5

How does TSIG authenticate name servers in order to perform secured zone transfers?

a) Both servers mutually verify their X509 certificates.
b) Both servers use a secret key that is shared between the servers.
c) Both servers verify appropriate DANE records for the labels of the NS records used to delegate the transferred zone.
d) Both servers use DNSSEC to mutually verify that they are authoritative for the transferred zone.

Answer: b

Question: 6

Which DNS label points to the DANE information used to secure HTTPS connections to https://www.example.com/?

a) example.com
b) dane.www.example.com
c) soa.example.com
d) www.example.com
e) _443_tcp.www.example.com

Answer: e

Question: 7

What is the purpose of IP sets?

a) They group together IP addresses that are assigned to the same network interfaces.
b) They group together IP addresses and networks that can be referenced by the network routing table.
c) They group together IP addresses that can be referenced by netfilter rules.
d) They group together IP and MAC addresses used by the neighbors on the local network.
e) They group together IP addresses and user names that can be referenced from /etc/hosts.allow and /etc/hosts.deny

Answer: c

Question: 8

Linux Extended File Attributes are organized in namespaces. Which of the following names correspond to existing attribute namespaces?

(Choose THREE correct answers.)

a) default
b) system
c) owner
d) trusted
e) user

Answer: b, d, e

Question: 9

Given a proper network and name resolution setup, which of the following commands establishes a trust between a FreeIPA domain and an Active Directory domain?

a) ipa trust-add --type ad addom --admin Administrator --password
b) ipa-ad –add-trust --account ADDOM\Administrator--query-password
c) net ad ipajoin addom –U Administrator -p
d) trustmanager add –-domain ad: //addom --user Administrator –w
e) ipa ad join addom -U Administrator -w

Answer: a

Question: 10

Which of the following sections are allowed within the Kerberos configuration file krb5.conf?

(Choose THREE correct answers.)

a) [plugins]
b) [crypto]
c) [domain]
d) [capaths]
e) [realms]

Answer: a, d, e

Study Guide to Crack LPI LPIC-3 303-200 Exam:

- Getting details of the 303-200 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 303-200 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the LPI provided training for 303-200 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 303-200 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 303-200 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for 303-200 Certification

Make EduSum.com your best friend during your LPI Security - 303 exam preparation. We provide authentic practice tests for the 303-200 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual 303-200 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the 303-200 exam.

Start Online practice of 303-200 Exam by visiting URL
https://www.edusum.com/lpi/303-200-lpi-security-303